

TABLE OF CONTENTS

| <u>SECTION</u> | <u>PAGE</u> |
|---|----------------------|
| 5.6 Generic Encryption Device Requirements..... | 1435 |
| 5.6.1 Introduction..... | 1435 |
| 5.6.2 Encryption Products Overview | 1436 1435 |
| 5.6.3 Minimum Requirements | 1439 |
| 5.6.3.1 Flexible and Robust Security | 1439 |
| 5.6.3.2 Interfaces..... | 1439 |
| 5.6.3.3 Operational Management..... | 1439 |
| 5.6.3.4 Zeroization | 1440 |
| 5.6.3.5 Maintainability and Serviceability..... | 1441 1440 |
| 5.6.3.6 Data Recovery..... | 1441 |
| 5.6.3.7 External Interfaces | 1441 |
| 5.6.3.8 Programmability | 1441 |
| 5.6.3.9 Performance | 1441 |
| 5.6.3.10 Network Operations | 1442 1441 |
| 5.6.3.11 Key Management..... | 1442 |
| 5.6.4 Operational Control over Features and Capabilities Management..... | 1442 |
| 5.6.5 General GCIRD Specification Language | 1442 |
| 5.6.6 Relationships Among Unified Capabilities Requirements Documents | 1442 |
| 5.6.6.1 Assumptions and Dependencies | 1443 1442 |
| 5.6.6.2 Applicable Documents..... | 1443 |

LIST OF FIGURES

| <u>FIGURE</u> | <u>PAGE</u> |
|--|--------------------|
| 5.6-1 ECU Overview Diagram..... | 1436 |
| 5.6-2 Example HAIPE Application Diagram..... | 1437 |
| 5.6-3 Example LEF Application Diagram | 1438 |

LIST OF TABLES

| <u>TABLE</u> | <u>PAGE</u> |
|--|----------------------|
| 5.6-1 Core Government Documents..... | 1444 1443 |
| 5.6-2 HAIPE Government Documents..... | 1445 |
| 5.6-3 LEF Government Documents | 1446 |
| 5.6-4 Core Non-Government Documents | 1446 |
| 5.6-5 HAIPE Non-Government Documents | 1447 |
| 5.6-6 LEF Non-Government Documents | 1447 |

5.6 GENERIC ENCRYPTION DEVICE REQUIREMENTS

5.6.1 Introduction

This section presents a system overview of End Cryptographic Units (ECUs) encryption products, e.g., HAIPE and Link Encryptor Family (LEF). Subordinate subsections of this section provide the core interoperability requirements applicable to each HAIPE and LEF cryptographic device. The requirements are extracted from the Generic Cryptographic Interoperability Requirements Document (GCIRD), Version 1.3, dated 07 January 2008. The GCIRD was developed by Subject Matter Experts (SMEs) and provides DoD vetted requirements critically needed for JITC testing and certification of Information Assurance products developed under the Commercial Communications Security (COMSEC) Evaluation Program (CCEP). The development of the GCIRD was requested by the Joint Staff.

Interoperability and Supportability needs are addressed in CJCSI 6212.01D, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS). CJCSI 6212.01D establishes policies and procedures for developing, coordinating, reviewing, and approving interoperability and supportability needs, as well as certifying that those needs have been met. The GCIRD provides a set of standards to address interoperability engineering and testing of CCEP products. The purpose of the GCIRD is to provide a coordinated and testable set of requirements to ensure interoperability certification of modernized ECUs.

The GCIRD establishes interoperability requirements to guide product development so that they can achieve Joint interoperability certification. The scope of these requirements is limited to NSA-approved CCEP products and other COMSEC products not covered by traditional capabilities documents intended for DoD. The GCIRD is a dynamic document and will be maintained and updated on an annual basis or as required by the Joint Services Cryptographic Modernization Working Group (JSCMWG) Cryptographic Products Testing (CPT) Integrated Product Team (IPT). At the same time as the GCIRD is updated, this section of the UCR will be updated to remain consistent with the GCIRD.

Note: Use of Cryptographic Devices from Approved Produces List (APL). Service Components and organizations shall confirm with their respective Chief Information Officer (CIO) which cryptographic devices are appropriate for use on their communications networks. Devices on the UC APL must be internally validated by the services and components for use at the Service or component level. The UC APL supports the Unified Capabilities or Defense Information System Network (DISN), it does not replace a requirement for the services/components to obtain authorization from their service specific CIO prior to procurement.

Devices that have not met service specific requirements must be evaluated for appropriateness prior to acquisition and installation on any DoD Network, tactical or strategic.

5.6.2 Encryption Products Overview

The ECUs are components of information systems that provide security services, which may include confidentiality, identification and authentication, integrity, and non-repudiation, to the overall system. Typically, the ECU is integrated with other components to provide the overall security required for the system. As such, neither the ECU nor the encryption function provided is a standalone system. [Figure 5.6-1](#), ECU Overview Diagram illustrates the use of the ECU in a system.

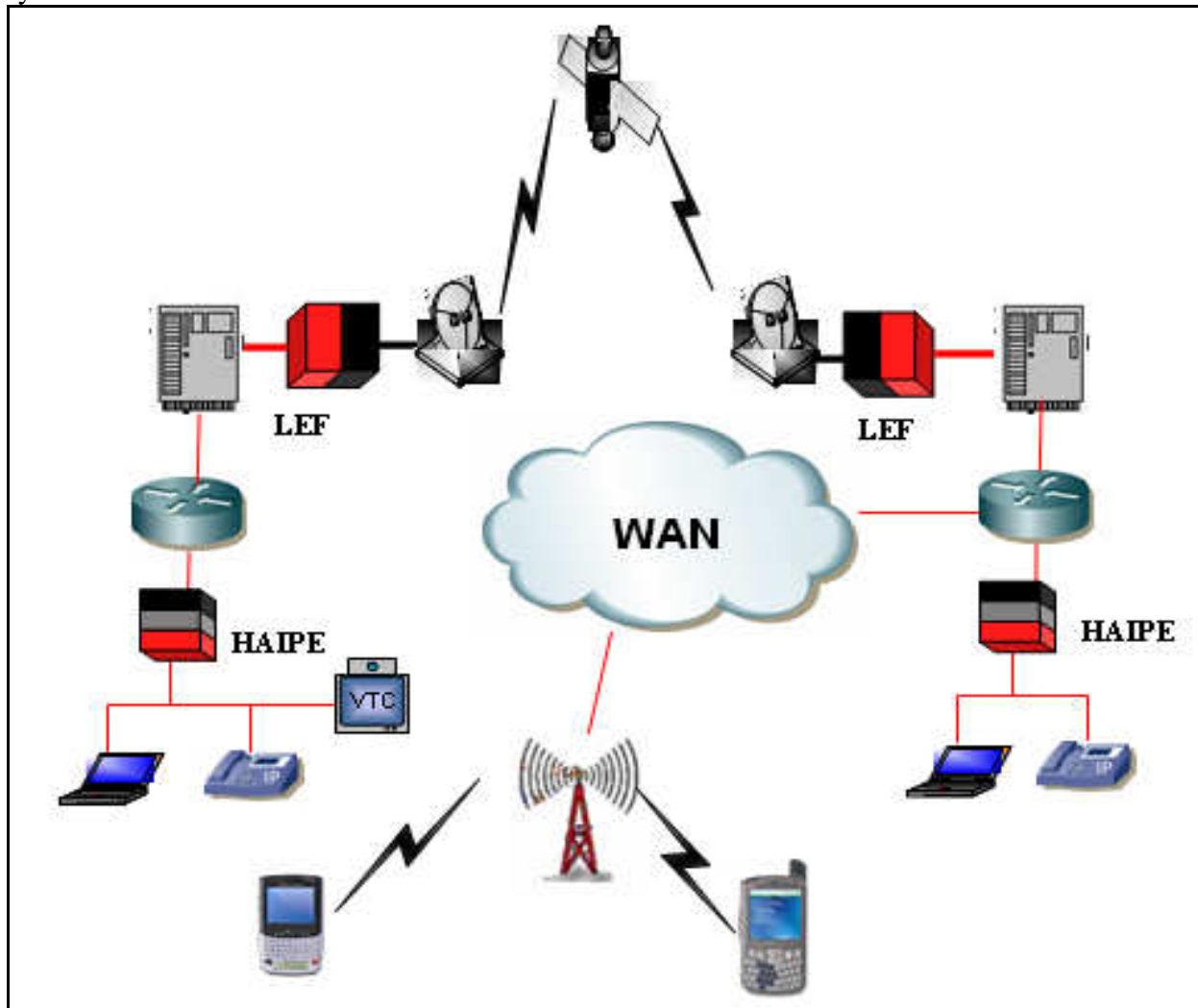


Figure 5.6-1. ECU Overview Diagram

A HAIPE is a programmable IP Information Security (INFOSEC) device with traffic protection, networking, and management features that provide Information Assurance services for IPv4 and IPv6 networks. The HAIPE(s) that are version 3.x compliant meet the DoD mandate for IPv6 compatibility and the goals of the Cryptographic Modernization Initiative (CMI), and are a key component of the GIG Vision. The HAIPE device is designed to provide confidentiality,

integrity, and authentication services for IP traffic for Deployable and Fixed network applications. The HAIPE enables secure transmission across WANs via IP packet encryption to compatible destination network security devices where decryption takes place. [Figure 5.6-2](#), Example HAIPE Application Diagram, provides an example of HAIPE implementation within a WAN.

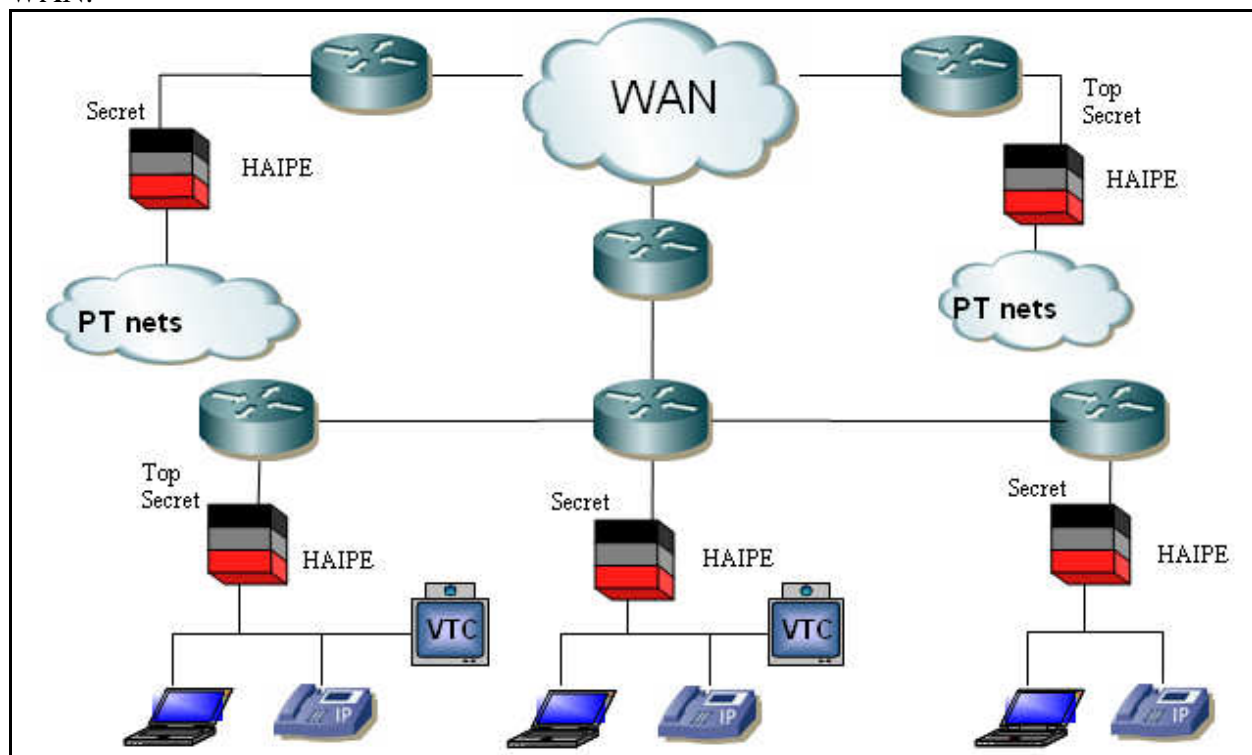


Figure 5.6-2. Example HAIPE Application Diagram

Design requirements are captured and promulgated in the HAIPE Interoperability Specification (IS). The HAIPE IS provides interoperability requirements for the following interconnections:

- HAIPE Device to HAIPE Device
- HAIPE Device to Key Management Infrastructure (KMI)
- HAIPE Device to Security Management Infrastructure (SMI)
- HAIPE Device to Network Component Infrastructure (NCI)

A HAIPE compliancy, (a.k.a., “HAIPE Interoperability Certification”) is granted by the NSA for a COMSEC device that complies with HAIPE IS v3.0.x. Whereas JITC interoperability Certification deals with interoperability as defined by CJCSI 6212.01D, JITC certification will not be granted until the device is Type-1 certified by NSA. The HAIPE compliance is met by meeting the requirements in the Networking Core and Traffic Protection Core Specifications, plus the three Classified cryptography specifications (Suite A, Suite B, and Legacy), and any Extension Specifications. In HAIPE IS 3.1.x, the Networking Core and Traffic Protection Core Specifications have been combined into a single Core specification.

The LEF ECUs are backward compatible with their legacy family members of equipment to the degree necessary to support continuous operations. Although LEF requirements will vary based on implementation, JITC interoperability testing is still required. Additional testing may be required based on individual Services requirements.

The LEF Specification establishes the detailed cryptographic requirements and basic functional, performance, and security requirements of the Cryptographic Modernization (CM) version of the LEF link/bulk ECUs. This section incorporates the appropriate LEF Specification requirements to provide a sufficiently detailed baseline set of requirements while allowing vendors design flexibility as to the form, fit, and additional functionality of the resulting ECUs. [Figure 5.6-3](#) illustrates the use of the LEF in a system.

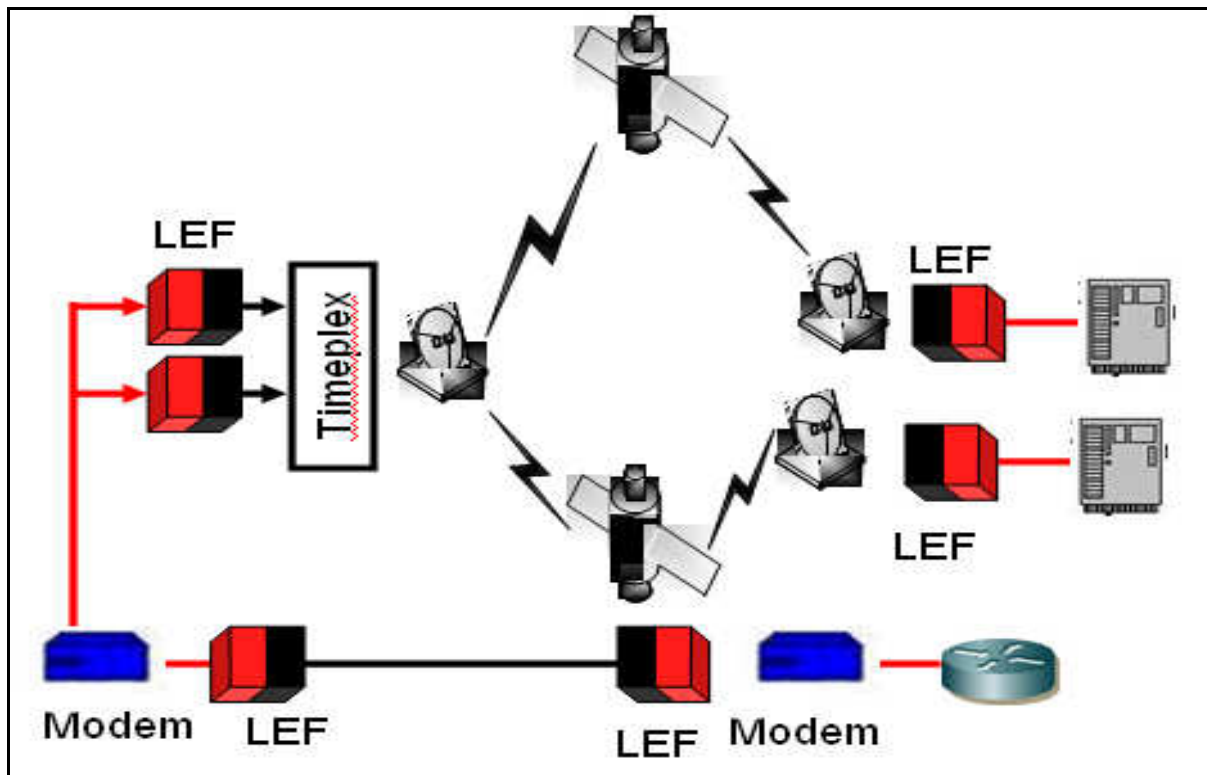


Figure 5.6-3. Example LEF Application Diagram

5.6.3 Minimum Requirements

The following subsections present minimum ECU requirements organized by operational capability category.

5.6.3.1 *Flexible and Robust Security*

[Required: HAIPE and LEF] The ECUs shall have the capability to be loaded and configured with legacy algorithms and modes to provide legacy-interoperable encryption services with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0215).

[Required: HAIPE and LEF] The ECUs shall have an inherent Information Assurance capability to ensure information and process integrity (during storage, processing, transmission, and presentation) to prevent unauthorized or unintended changes with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0249).

5.6.3.2 *Interfaces*

[Required: HAIPE and LEF] The ECUs shall be capable of loading and accepting keying material (KEYMAT) from NSA-approved key fill devices with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0295).

[Required: HAIPE and LEF] The ECUs shall include a DS-101 cryptographic fill port interface IAW EKMS 308 with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0149).

[Required: LEF] The LEF ECUs shall implement data interfaces that conform to the EIA-530 standard. Additional details associated with the interface parameters are defined in the Generic Cryptographic Interoperability Requirements Database (ID0635).

[Required: LEF] The LEF ECUs shall implement data interfaces that conform to the RS-232 standard. Additional details associated with the interface parameters are defined in the Generic Cryptographic Interoperability Requirements Database (ID0661).

5.6.3.3 *Operational Management*

[Required: HAIPE and LEF] The ECUs shall recover last known, good operational state/settings after loss of primary power with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0210).

[Conditional: HAIPE and LEF] The ECUs should have the capability to provide data to management devices to generate user defined high-level operational status reports with 90 percent reliability.

If a HAIPE or LEF implements this feature, it shall perform as specified in the Generic Cryptographic Interoperability Requirements Database (ID0377).

[Required: HAIPE] The HAIPE(s) shall not preclude operation over low bandwidth networks as low as 2.4 kB/s with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0237).

[Conditional: HAIPE] The HAIPEs should have the capability to execute the In-Line Network Encryptor (INE) Management command and control function with 90 percent reliability.

If a HAIPE implements this feature, it shall perform as specified in the Generic Cryptographic Interoperability Requirements Database (ID0320).

[Conditional: HAIPE] The HAIPEs should have the capability to execute the Backup Remote Management (RM) command and control function with 90 percent reliability.

If a HAIPE implements this feature, it shall perform as specified in the Generic Cryptographic Interoperability Requirements Database (ID0325).

[Required: LEF] The LEF ECUs shall be capable of operating with legacy Time Division Multiple Access (TDMA) architectures for networked data exchange with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0029).

[Required: LEF] The LEF ECUs shall be able to automatically recover security connections after loss of power on one end or both ends of a channel with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0639).

5.6.3.4 Zeroization

[Required: HAIPE and LEF] The ECUs shall prevent the accidental deletion of all loaded operational key with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0591).

5.6.3.5 Maintainability and Serviceability

[Required: HAIPE and LEF] New software releases shall, as a minimum, be backward compatible with the previous NSA-certified version of software with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0214).

[Required: LEF] The LEF ECUs shall provide autophase if interoperable with KG-84C with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID044).

5.6.3.6 Data Recovery

[Required: HAIPE] The HAIPE(s) shall be able to recover security associations after loss of power on one end or both ends of the link with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0211).

5.6.3.7 External Interfaces

[Required: HAIPE] The HAIPE(s) shall adhere to standard commercial interfaces (e.g., Ethernet, Fast Ethernet, Gigabit Ethernet, or 10Gigabit Ethernet). Additional details associated with the interface parameters are defined in the Generic Cryptographic Interoperability Requirements Database (ID0223).

[Required: HAIPE] The HAIPE(s) devices shall be compatible with network components such as routers and hosts in common usage within the GIG Information Assurance architecture with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0226).

5.6.3.8 Programmability

[Required: HAIPE] The HAIPE(s) shall be capable of being reprogrammed with updated cryptographic software and algorithms with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0450).

5.6.3.9 Performance

[Required: HAIPE] The HAIPE(s) shall operate over connections to satellite links that experience delays of up to two seconds aggregate with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0235).

5.6.3.10 Network Operations

[Required: HAIPE] When subjected to 70 percent or greater of rated throughput, HAIPE(s) shall maintain secure communications without interruption (i.e., without reboot) with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0166).

5.6.3.11 Key Management

[Required: LEF] The LEF ECUs shall have Over-the-Air-Rekey (OTAR) capability with 90 percent reliability as specified in the Generic Cryptographic Interoperability Requirements Database (ID0022).

5.6.4 Operational Control over Features and Capabilities Management

The GCIRD augments CCEP required documentation such as the product/system-specific Telecommunications Security Requirements Document (TSRD) and Information Assurance Security Requirements (IASRD).

5.6.5 General GCIRD Specification Language

The GCIRD uses non-UCR 2008 terminology to define the weighting factors incorporated into the ECU requirement specifications. This differs from the language used in Section 5.1.4, General Requirement Language. The mapping from GCIRD to UCR terminology is presented in the following paragraphs:

- The term “SHALL” designates the most important weighting level; that is, mandatory. In Section 5.6, this requirement has been mapped to the term “REQUIRED.”
- The term “SHOULD” designates requirements, which are requested but are not mandatory. In Section 5.6, this requirement has been mapped to the term “CONDITIONAL.”

5.6.6 Relationships among UC Requirements Documents

The following assumptions, dependencies, and references pertain to the ECU products described throughout Section 5.6 and amplify the relationships among UCR documents discussed in Section 5.1.5, AS-SIP Requirement Adheres to IETF Specification Language.

5.6.6.1 Assumptions and Dependencies

The following identifies all assumptions and dependencies developed by the Ad Hoc Working Group (AHWG) regarding external factors that may affect interoperability and acquisition processes supported by the GCIRD.

- Policy (i.e., CJCSI 6212) will be modified as appropriate.
- DoD testing community, to include respective service test commands, will accept and use the GCIRD.
- DOD Architecture Framework (DODAF) products and NR-KPP will be addressed in the Joint Capabilities Integration and Development System (JCIDS) documentation of systems utilizing CCEP products.
- The GCIRD is a living document managed by a CPT IPT established under charter and authority of the JSCMWG and updated/changed yearly or as required.
- SCIP products are covered elsewhere in UCR 2008.

5.6.6.2 Applicable Documents

The GCIRD provides interoperability requirements for product development and Joint interoperability certification. The scope of these requirements is limited to approved NSA CCEP products and other COMSEC products not covered by traditional capabilities documents intended for DoD. The GCIRD and underlying database will also serve as a cryptographic requirements reference document readily available to the testing community, program managers across DoD, and commercial vendors. This document identifies the core interoperability requirements for cryptographic products and those unique requirements common to individual cryptographic families.

The GCIRD is for use by all DoD Components (including COCOMs, Services, and Agencies) and commercial vendors to aid in development of ECUs. It applies to development of new cryptographic products as well as major hardware and software upgrades for existing CryptoMod-compliant products. The GCIRD applies to cryptographic equipment/devices procured for installation in the GIG. For Joint interoperability testing and certification, this document takes precedence over the explicit or implicit requirements of subsidiary or reference documents, standards, and specifications unless applicable, validated JCIDS documents already exist.

Section 5.6 – Generic Encryption Device Requirements

Tables 5.6-1 through 5.6-6 provide a detailed listing of the applicable Government and non-Government documents. These tables were extracted from the Draft GCIRD, Version 1.3, dated January 07, 2008.

Table 5.6-1. Core Government Documents

| DOC ID | NAME | DATE |
|---------------------------|--|-------------|
| NSA/CSS POLICY NUMBER 3-9 | Cryptographic Modernization Initiative Requirements for Type 1 Cryptographic Products | 28 Mar 2003 |
| CM MA ICD | Cryptographic Modernization Mission Area Initial Capabilities Document | 14 Aug 04 |
| MIL-STD-1275D | Department of Defense Interface Standard Characteristics of 28 Volt dc Electrical Systems in Military Vehicles | 29 Aug 2006 |
| MIL-STD-961E | Department of Defense Standard Practice Defense and Program-Unique Specifications Format and Content | 01 Aug 2003 |
| MIL-STD-167-1A | Department of Defense Test Method Standard Mechanical Vibrations of Shipboard Equipment | 02 Nov 2005 |
| MIL-HDBK-502 | DOD Handbook Acquisition Logistics | 30 May 1997 |
| EKMS 217 | EKMS Benign Techniques Specification Rev G | 21 Dec 2001 |
| EKMS 322B | EKMS FIREFLY Specification (SECRET) | 05 Apr 2002 |
| EKMS 218 | Generic Rekey Front End System Requirements | 13 Dec 2001 |
| MIL-STD-1399C (NAVY) | Interface Standard For Shipborne Systems | 02 Feb 1988 |
| DODD 4630.5 | Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) | 05 May 2004 |
| CJCSI 6212.01D | Interoperability and Supportability of Information Technology and National Security Systems | 08 Mar 2006 |
| CJCSI 3170.01E | Joint Capabilities Integration and Development System | 11 May 2005 |
| EKMS 308 | Key Distribution Functional Standard Rev D SCN-2 | 23 Mar 2004 |
| | KMI CI-2 CDD | 17 Feb 2005 |
| MIL-HDBK-5400 | Military Handbook Airborne General Guidelines for Electronic Equipment | 30 Nov 1995 |
| MIL-HDBK-454A | Military Handbook General Guidelines for Electronic Equipment | 03 Nov 2000 |
| MIL-S-901D (NAVY) | Military Specification Requirements for Shock Tests, H.I. (High-Impact) Shipboard Machinery, Equipment, and Systems | 17 Mar 1989 |
| CNSSI 4009 | National Information Systems Security INFOSEC Glossary | Sep 2000 |
| DODI 5000.2 | Operation of the Defense Acquisition System | 12 May 2003 |
| CJCSM 3170.01B | Operation of the Joint Capabilities Integration and Development System | 11 May 2005 |
| | P ³ Generation & Distribution Specification for Foreign Interoperability In-Line Network Encryptors (INE), v2 | 20 Oct 2005 |
| DODI 4630.8 | Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) | 30 Jun 2004 |
| NIST SP 800-56A | Recommendation for Obtaining Assurances for Digital Signature Application | Apr 2006 |

Section 5.6 – Generic Encryption Device Requirements

| DOC ID | NAME | DATE |
|---------------|---|-------------|
| MIL-HDBK-217F | Reliability Prediction of Electronic Equipments | 28 Feb 1995 |
| CNS 4005 | Safeguarding Communications Security Facilities and Materials | Aug 1997 |
| KMI 3003 | Sender Intermediary Receiver (SIR) Model | 29 Oct 2005 |
| | TECOM Test Operations Procedure (TOP) 1-2-511 | 29 Dec 1989 |
| DODD 5000.1 | The Defense Acquisition System | 24 Nov 2003 |

Table 5.6-2. HAIPE Government Documents

| DOC ID | NAME | DATE |
|-----------|---|-------------|
| | HAIPE (Version 1.35) Remote Manager Test Plan v1.1 | 22 Feb 2006 |
| | HAIPE Interoperability Specification (IS) 1.3.5 | 11 May 2004 |
| | HAIPE Interoperability Specification 3.1.0 | 31 Dec 2006 |
| | HAIPE IS 3.1 Auto Security Association Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Gateway Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Generic Discovery Client Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Implicit Peer Enclave Prefix Discovery Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Legacy Discovery Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Legacy Encapsulating Security Payload Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Reachability Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Remote Configuration and Monitor Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Remote Provisioning Authority Extension | 31 Dec 2006 |
| | HAIPE IS 3.1 Remote Provisioning Extension | 31 Dec 2006 |
| DISA/JITC | High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Test Plan | Mar 2006 |
| DISA/JITC | High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Test Report | Aug 2006 |
| | TRADOC Futures Center Reliability and Maintainability (R&M) ANALYSIS for the High Assurance Internet Protocol Encryptor (HAIPE) | 22 Aug 2005 |

Table 5.6-3. LEF Government Documents

| DOC ID | NAME | DATE |
|------------|--|-------------|
| | KIV-7M Encryption Device Release 1.0 Interoperability Assessment Plan | Jul 2006 |
| | LEF Key Specification, Rev E | 01 Nov 06 |
| | LEFCIS Classified Appendix | 09 May 2006 |
| NSA 03-01A | Link Encryptor Family (LEF) Cryptographic Interoperability Specification Version 2.1.0 | 09 May 2006 |
| | TRADOC Futures Center Reliability and Maintainability (R&M) Analysis for the Link Encryptor Family (LEF) | 22 Aug 2005 |

Table 5.6-4. Core Non-Government Documents

| DOC ID | NAME | DATE |
|------------------------------|---|-------------|
| ANSI/EIA-310-D-92 | Cabinets, Racks, Panels and Associated Equipment. American National Standards Institute (ANSI)/Electronic Industries Association (EIA) Standard | Sep 1992 |
| ITU P.Imp563 | Implementers Guide for ITU-T Recommendation P.563 | |
| RFC 3647 | Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework | Nov 2003 |
| ITU-T Recommendation P.800.1 | Mean Opinion Score (MOS) Terminology | Mar 2003 |
| ITU-T Recommendation P.800 | Methods for subjective determination of transmission quality (formerly P. 80) | 1996 |
| ITU-T Recommendation P.563 | Single-ended method for objective speech quality assessment in narrow-band telephony applications. | 2004 |
| ASME Y14.35M | This standard defines the practices for revising drawings, associated documentation, and establishes methods for identification and recording revisions. The revision practices of this Standard apply to any form of original drawing and associated documentation. | 08 Dec 1997 |
| ASME Y14.24 | This standard defines the types of engineering drawings most frequently used to establish engineering requirements. It describes typical applications and minimum content requirements. Drawings for specialized engineering disciplines (e.g., marine, civil, construction, optics) are not included in this Standard. | 01 Jan 1999 |
| ASME Y14.100 | This standard establishes the essential requirements and reference documents applicable to the preparation and revision of engineering drawings and associated lists. It is essential that this standard be used with ASME Y14.24, ASME Y14.34M, and ASME Y14.35M. | 01 Jan 2004 |

Section 5.6 – Generic Encryption Device Requirements

| DOC ID | NAME | DATE |
|--------------|--|-------------|
| ASME Y14.34M | This standard establishes the minimum requirements for the preparation and revision of parts lists, application lists, data lists, and index lists. In addition, this standard presents certain options that may be incorporated into parts lists, data lists, index lists, application lists, indented data lists, and wire lists at the discretion of the design activity. | 01 Jan 1996 |
| | Universal Serial Bus (USB) Specification Version 2.0 | 07 Dec 2000 |
| RFC 4108 | Using CMS to Protect Firmware Packages | Aug 2005 |

Table 5.6-5. HAIPE Non-Government Documents

| DOC ID | NAME | DATE |
|----------|---------------------------------------|----------|
| RFC 3414 | User-Based Security Model for SNMP V3 | Dec 2002 |
| RFC 3415 | View-Based Access Control Model SNMP | Dec 2002 |

Table 5.6-6. LEF Non-Government Documents

| DOC ID | NAME | DATE |
|---------|--|------|
| EIA-530 | Electronics Industries Alliance (EIA) Standard for the Interconnection of DTE and DCE Employing Serial Binary Data Interchange with Control Information Exchanged on Separate Control Circuits | |
| RS-232 | Recommended Standard 232 for Serial Binary Data Signals Connecting Between a DTE and a DCE | |

THIS PAGE INTENTIONALLY LEFT BLANK